DCSO

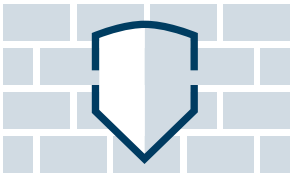
WHITEPAPER

Jede Minute zählt.

Warum Detection nicht genügt – und wie strategische MDR Ihre Souveränität sichert.

Executive Summary

Cyberangriffe auf kritische Infrastrukturen haben sich seit 2024 deutlich verschärft, insbesondere in den Sektoren Energie, Gesundheitswesen und öffentliche Verwaltung [13] [4]. 68 % der Angriffe nutzen inzwischen KI-gestützte Methoden, 42 % werden staatlichen Akteuren zugeschrieben [7] [13]. Das Volumen von Ransomware-Angriffen hat sich verdoppelt, mit durchschnittlichen Lösegeldforderungen von 1,5 Mio. Euro [29].



Traditionelle Sicherheitsmaßnahmen erkennen durchschnittlich nur 63 % moderner Angriffe, bei einer mittleren Erkennungszeit von 207 Tagen [6]. Im Vergleich dazu reduzieren **24/7/365 Managed Detection and Response (MDR)**-Dienste die Verweildauer von Angreifern von durchschnittlich 212 auf 48 Tage und identifizieren 91 % der Vorfälle innerhalb der ersten Stunde – was eine unmittelbare Abwehr ermöglicht [DCSO-interne Analysen, 2025].

MSSP-Lösungen mit eigener Incident Response, kontinuierlich betriebenem Security Operations Center (SOC) und integrierter Threat Intelligence ermöglichen darüber hinaus Kosteneinsparungen von bis zu 45 % bei gleichzeitig deutlich verbesserter Sicherheitslage [4] [28].

Einführung

Die digitale Transformation hat die Angriffsfläche für Cyberkriminalität erheblich erweitert – besonders im Bereich kritischer Infrastrukturen, mittelständischer Unternehmen und Behörden [13]. Die aktuelle Bedrohungslage ist geprägt von einer deutlichen Zunahme komplexer Angriffe, die zunehmend durch staatliche Akteure gefördert und mit KI-gestützten Methoden durchgeführt werden [3] [7].

Traditionelle Sicherheitsansätze stoßen hier an ihre Grenzen: Sie erkennen in der Regel nur bekannte Bedrohungen und bieten keine durchgehende Echtzeit-Überwachung [6]. Vor diesem Hintergrund gewinnt der Einsatz eines **Managed Security Service Providers (MSSP)** mit eigener Incident Response, einem **24/7/365** betriebenen SOC und integrierter Threat Intelligence an strategischer Bedeutung. Diese Kombination ermöglicht nicht nur eine schnellere Erkennung und Reaktion auf Bedrohungen, sondern auch eine kosteneffiziente, maßgeschneiderte Sicherheitsstrategie, die unterbrechungsfrei Risiken minimiert [4].

Die aktuelle Cyber-Bedrohungslandschaft und ihre Herausforderungen

Der BSI-Lagebericht 2024 weist täglich über 309.000 neu registrierte Schadprogramme in Deutschland aus – ein Anstieg von 26 % im Vergleich zum Vorjahr [13]. Besonders betroffen sind kritische Infrastrukturen wie Energieversorgung, Gesundheitswesen und öffentliche Verwaltung. Diese Sektoren sind nicht nur essenziell für die nationale Sicherheit, sondern auch besonders attraktiv für Cyberkriminelle, die durch Ransomware, Spionage und Sabotage hohe finanzielle und strategische Gewinne erzielen wollen [14].

Ein besorgniserregender Trend ist der zunehmende Einsatz von KI-gestützten Angriffsmethoden, die in 68 % der Fälle zum Einsatz kommen und klassische Schutzmaßnahmen umgehen [7] [13]. Rund 42 % der Angriffe auf kritische Infrastrukturen stammen von staatlichen Akteuren, die über erhebliche Ressourcen und hochentwickelte Techniken verfügen [1]. Die durchschnittliche Verweildauer von Angreifern in kompromittierten Systemen liegt bei 212 Tagen, was die Dringlichkeit schneller Erkennung und Reaktion unterstreicht [6].

Zudem hat sich das Volumen von Ransomware-Angriffen verdoppelt, mit durchschnittlichen Lösegeldforderungen von 1,5 Mio. Euro [29]. Diese Entwicklungen verdeutlichen, dass die Bedrohungslage komplexer, dynamischer und gefährlicher geworden ist – und dass herkömmliche Sicherheitsansätze allein nicht mehr ausreichen.

Die drei Säulen strategischer MDR:
Souveränität, bedarfsoptimierte Lösungen und 24/7/365-Schutz

Digitale Souveränität

Digitale Souveränität – die Fähigkeit, Daten und IT-Infrastrukturen eigenständig, sicher und rechtskonform zu kontrollieren – ist insbesondere für kritische Infrastrukturen und Behörden von zentraler Bedeutung [31] [32].
Eine aktuelle Bitkom-Studie zeigt: 89 % der deutschen Unternehmen bevorzugen, wenn möglich, „Made in Germany"-Lösungen. Diese senken durch ausschließlich lokale Datenspeicherung die Compliance-Kosten um bis zu 35 %, erhöhen die Reaktionsgeschwindigkeit und erfüllen höhere Datenschutzstandards [32] [33].
Ein führender deutscher Automobilhersteller entschied sich beispielsweise für die Implementierung einer vollständig lokalen MSSP-Lösung. Ergebnis: Compliance-Kosten um 30 % gesenkt, Reaktionszeiten auf Sicherheitsvorfälle von durchschnittlich 48 Stunden auf unter zwei Stunden reduziert [34].
Zum Erreichen dieser Ziele kommen in Deutschland entwickelte Sensorik und Edge Nodes bzw. embedded SIEMs zum Einsatz. Diese überwachen kontinuierlich Netzwerkströme und Log-Daten, erkennen verdächtige Ereignisse in Echtzeit („Live-Matching") und verarbeiten sämtliche Daten lokal – die Datenhoheit bleibt vollständig beim Kunden. Die Speicherdauer lässt sich flexibel anpassen, nicht relevante Daten werden automatisch gelöscht, was DSGVO- und Betriebsrats-Konformität sicherstellt.

Die Angriffserkennung basiert auf German Security Engineering:

- Mustererkennung mit aktuellen IDS-Signaturen
- IoC-Matching gegen bekannte Bedrohungsindikatoren (z. B. Domains, Hostnamen, URLs)
- Heuristik-basierte Analysen für komplexe Angriffsmuster wie C2-Beaconing
- Use-Case-basierte Regeln im embedded SIEM, standardisiert oder kundenspezifisch angepasst

Ein weiterer Vorteil ist das **Retro-Matching**: Gespeicherte Metadaten werden lokal auf den Edge Nodes vorgehalten und bei neuen Bedrohungsinformationen (IoC) nachträglich durchsucht – ohne Datenabfluss ins Ausland. Für forensische Analysen ermöglicht das **Retro-Hunting** gezielte Abfragen durch DCSO-Analysten, exklusiv auf deutscher Infrastruktur. So lassen sich etwa Lateral-Movement-Angriffe nachvollziehen, ohne Abhängigkeit von internationalen Anbietern. Die gesamte Analysekette – von der Echtzeiterkennung bis zur Incident Response – bleibt unter deutscher Kontrolle. Als beim BSI gelisteter APT-Response-Dienstleister bietet die DCSO zudem geprüfte und zertifizierte Reaktionsfähigkeit [35].

Bedarfsoptimierte Lösungen

72 % der Unternehmen benötigen maßgeschneiderte Sicherheitslösungen, die auf ihre spezifischen Anforderungen abgestimmt sind [27]. Qualitativ hochwertige MSSP-Lösungen kombinieren menschliche Expertise mit automatisierten Prozessen und können so Sicherheitskosten signifikant reduzieren – im Schnitt um bis zu 45 % [28].
Ein Beispiel aus dem Gesundheitssektor: Durch die Implementierung einer branchenspezifisch zugeschnittenen MSSP-Lösung sanken die Sicherheitskosten um 40 %, während die Erkennungsrate von Vorfällen auf 95 % stieg [29] [30].
Passoptimierte Strategien schaffen zudem Investitionssicherheit und ermöglichen die Weiternutzung bestehender Infrastruktur. Oft beruhen Kundenumgebungen auf historisch gewachsenen, vertrauten Insellösungen. Statt diese vollständig zu ersetzen, werden sie behutsam unter einem übergeordneten MDR-Schutzschirm integriert. Herstellerunabhängigkeit stellt sicher, dass bestehende Investitionen geschützt bleiben.

Der optimale 10-Punkte-Onboarding-Prozess umfasst in der Praxis:

1. Workshop mit Risikobewertung und Priorisierung kritischer Systeme/Daten
2. Modellierung von Optimierungspotential und Weiterbetrieb der IST-Umgebung
3. Definition relevanter Erkennungsszenarien und Use-Cases Identifizierung aller relevanten Protokollquellen
4. Identifizierung aller relevanten Protokollquellen
5. Integration der Quellen in Edge Nodes und Planung zusätzlicher Netzwerksensorik

6. Implementierung von Use-Cases und Definition des „Normalbetriebs“

7. Testphase zur Validierung der Anomalieerkennung

8. Abstimmung der Use-Cases und Dokumentation für den SOC-Betrieb

9. Regelmäßige Analyse-Reviews mit einem dedizierten Analysten

10. Quartalsweise strategische Abstimmung zwischen Senior Director Cyber Defense und Geschäftsführung

Dieser strukturierte Ansatz maximiert die Sichtbarkeit für SOC-Analysten, erhöht die Reaktionsgeschwindigkeit und gewährleistet eine präzise Anpassung an die Kundenumgebung.

24/7/365-Schutz

Im Ernstfall zählt bei Cyberangriffen jede Minute. Kontinuierliches Monitoring und eine schnelle Reaktion sind entscheidend, um Schäden zu minimieren. Unternehmen mit **24/7/365**-Überwachung erkennen Angriffe im Durchschnitt 75 % schneller als ohne kontinuierliche Kontrolle [16].
Aktive MDR-Services reduzieren die Verweildauer von Angreifern in Zielsystemen um bis zu 70 % und identifizieren bis zu 91 % der Vorfälle innerhalb der ersten Stunde [DCSO-interne Analysen, 2025].
Ein Praxisbeispiel aus einer Bundesbehörde: Nach Einführung einer **24/7/365-MDR-Lösung** sank die durchschnittliche Reaktionszeit auf Vorfälle von 72 Stunden auf unter 30 Minuten – ein Wert, der durch Querschnittsanalysen im Kundenstamm verifiziert wurde. In einem dokumentierten Fall wurde an einem Wochenende gegen 02:00 Uhr ein kompromittierter Client isoliert, bevor sich der Angreifer lateral ausbreiten konnte. Diese schnelle Eindämmung wäre aus eigenen Ressourcen der Behörde nicht möglich gewesen.
Kontinuierliche, durchgehende Abwehr in Verbindung mit klar definierten Standard-Prozessen (Standard Operating Procedures - SOPs) ist somit ein zentraler Faktor für wirksame Schadensbegrenzung und Betriebskontinuität – gerade bei Angriffen außerhalb üblicher Arbeitszeiten.

Die Rolle von KI in der modernen Cyberabwehr

Künstliche Intelligenz (KI) hat die Bedrohungslandschaft im Cyberraum in den letzten Jahren grundlegend verändert – sowohl auf Angreifer- als auch auf Verteidigungsseite [7]. Angreifer nutzen KI, um Phishing-Kampagnen zu personalisieren, Schwachstellen automatisiert zu identifizieren und Zero-Day-Exploits in kürzester Zeit auszunutzen [3].
Gleichzeitig ermöglicht KI-betriebene Verteidigung eine bislang unerreichte Effizienz bei der Erkennung und Abwehr von Angriffen. So steigern KI-gestützte Threat-Detection-Systeme die Erkennungsrate um durchschnittlich 35 % und reduzieren Fehlalarme um 20 % [29].

In MDR-Umgebungen übernimmt KI vor allem repetitive, zeitkritische Aufgaben, etwa:

- Automatisierte Korrelation von Log-Daten und Netzwerkereignissen
- Priorisierung von Alerts anhand von Kontext- und Bedrohungsinformationen
- Erkennung bislang unbekannter Anomalien durch selbstlernende Modelle
- Unterstützung bei forensischen Analysen durch Mustervergleich in großen Datenmengen

Der entscheidende Faktor ist jedoch die **Mensch-Maschine-Kombination**: Während KI große Datenmengen schnell analysieren kann, bleibt die strategische Bewertung und Kontextualisierung von Bedrohungen Aufgabe erfahrener Analysten. In der Praxis entstehen so hybride SOC-Modelle, in denen KI den First-Level-Support automatisiert und menschliche Experten im Second- und Third-Level präzise Entscheidungen treffen [28].
Ein Fallbeispiel aus dem Finanzsektor verdeutlicht den Mehrwert: Ein MSSP integrierte KI-basierte Angriffserkennung in sein **24/7/365-SOC**. Die Anzahl kritischer Vorfälle, die innerhalb der ersten Stunde erkannt wurden, stieg von 64 % auf 92 %, während der Personalaufwand für die Erstbewertung von Alerts um 38 % sank [30].

KI in der Cyberabwehr ist damit kein Ersatz, sondern ein Multiplikator für menschliche Expertise – und ein zentrales Element moderner MDR-Strategien.

Risiken durch geopolitische Verwerfungen und außereuropäische Technologien

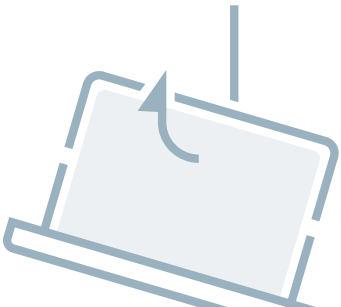
Die geopolitischen Spannungen und Konflikte haben erhebliche Auswirkungen auf die Cybersicherheitslandschaft. Russland nutzt den Cyber- und Informationsraum als Teil seiner hybriden Kriegsführung, um politische und militärische Ziele zu erreichen. Dazu gehören Cyberangriffe, Desinformationskampagnen und psychologische Operationen, die darauf abzielen, öffentliche Meinung zu beeinflussen, Unsicherheit zu verbreiten und die Stabilität westlicher Demokratien zu untergraben. Staatlich unterstützte Hackergruppen führen gezielte Angriffe auf kritische Infrastrukturen, Unternehmen und Behörden durch, während Propaganda und Falschinformationen über staatlich kontrollierte Medien und soziale Netzwerke verbreitet werden [7] [13] [19].

Auch Sicherheits- und IT-Dienstleister geraten zunehmend ins Visier, da ihre Dienste in kritischen Umgebungen automatisch eine höhere Glaubwürdigkeit genießen. Seit Angriffen wie auf SolarWinds oder die Colonial Pipeline haben feindliche Staaten und Cyberkriminelle die Ausnutzung von Schwachstellen in öffentlichen und privaten Netzwerken intensiviert, was zu einem weltweiten Anstieg von Cyberangriffen auf KRITIS um 30 % führte [7] [19].

Analysen zeigen zudem, dass für erfolgreiche Angriffe oft keine hochentwickelte Technologie notwendig ist: Iranische Hacker nutzten „simples“ Spear-Phishing gegen Wahlkampagnen und Regierungsmitarbeiter, China unterstützte die Gruppe Salt Typhoon bei Infiltration westlicher Parteiapparate, und Russland setzte unkoordinierte Botnetze ein, um soziale Medien zu manipulieren [7] [13] [19].

Darüber hinaus gibt es Hinweise darauf, dass weitverbreitete chinesische Hard- und Software möglicherweise versteckte „Kill Switches“ enthalten könnten, mit denen kritische Infrastrukturen wie Strom- und Wassersysteme abgeschaltet werden könnten. Diese Hintertüren könnten bereits zur Infiltration und potenziellen Sabotage genutzt werden. Auch bei anderen Zulieferernationen ist diese Gefahr nicht zu unterschätzen [13] [19].

Die Kombination aus geopolitischen Verwerfungen und mangelnder technologischer Souveränität erfordert eine robuste, koordinierte Antwort. Besonders souverän technologiegestützte Managed Detection & Response (MDR) kann hier einen fundamentalen Beitrag leisten und die Schutzmöglichkeiten für KRITIS und öffentliche Hand signifikant erhöhen, wie Erfahrungen aus dem Vereinigten Königreich, Singapur und Australien zeigen [7] [19].



Wirtschaftliche Vorteile und ROI von MDR

Managed Detection and Response (MDR) ist nicht nur ein Sicherheitsinstrument, sondern auch ein wirtschaftlicher Faktor. Studien zeigen, dass Unternehmen durch den Einsatz eines MDR-Service ihre durchschnittlichen Kosten pro Sicherheitsvorfall um bis zu 45 % senken können [28].

Diese Einsparungen entstehen durch eine Kombination aus kürzerer Verweildauer von Angreifern, reduzierten Ausfallzeiten und geringeren Kosten für forensische Untersuchungen.
Ein Unternehmen aus dem Energiesektor berichtete nach der Einführung einer **24/7/365-MDR-Lösung** von einer Verkürzung der mittleren Vorfallsdauer (Mean Time to Resolve, MTTR) um 72 %, was direkte Einsparungen in Millionenhöhe bedeutete [30]. Gleichzeitig wurden Compliance-Verstöße um 40 % reduziert, da Sicherheitslücken schneller erkannt und geschlossen wurden.

Neben den direkten Einsparungen verbessert MDR die Planbarkeit von IT-Sicherheitsbudgets. Statt unvorhersehbarer, hoher Ausgaben nach Vorfällen fallen feste monatliche Kosten an, die eine präzise Finanzplanung ermöglichen. Dieser **OPEX-Ansatz** ersetzt teure, reaktive CAPEX-Investitionen in Ad-hoc-Maßnahmen.

Der ROI eines MDR-Programms ergibt sich zudem aus der Vermeidung von Folgeschäden:

- **Verlust von Geschäfts- und Kundendaten** – potenziell existenzbedrohend für KMU
- **Reputationsschäden** – laut IBM dauert die Erholung vom Imageverlust nach einem Cybervorfall durchschnittlich 9 Monate [29]
- **Regulatorische Strafen** – etwa nach DSGVO-Verstößen, die Bußgelder von bis zu 4 % des weltweiten Jahresumsatzes vorsehen

Langfristig zeigt sich, dass Unternehmen mit MDR im Durchschnitt 38 % schneller wachsen, da sie Investitionen in Digitalisierung und Innovation mit geringerem Sicherheitsrisiko umsetzen können [7]. MDR steigert also nicht nur die Resilienz, sondern auch die Wettbewerbsfähigkeit.

Fähigkeiten eines MSSP
mit eigener Incident Response, 24/7/365 Managed SOC und Threat Intelligence

Ein Managed Security Service Provider (MSSP), der eigene Incident Response Teams, ein 24/7/365 betriebenes Security Operations Center (SOC) und integrierte Threat Intelligence bereitstellt, bietet Unternehmen und Behörden entscheidende Vorteile:

- **Echtzeit-Überwachung und schnelle Reaktion:** Kontinuierliche Beobachtung der IT-Infrastruktur, Erkennung von Anomalien und sofortige Reaktion auf Sicherheitsvorfälle rund um die Uhr [13] [19].
- **Proaktive Bedrohungserkennung, KI-gestützt:** Einsatz von KI und Machine Learning zur Erkennung bekannter und unbekannter Bedrohungen, einschließlich Zero-Day-Exploits, wobei agentenbasierte KI die menschlichen Analysten entlastet [7] [21].
- **Expertenanalyse und Incident Response:** Zugriff auf erfahrene Cybersicherheitsexperten für Analyse, Eindämmung und Behebung von Vorfällen – menschliche Erfahrung bleibt durch nichts zu ersetzen [19].
- **Threat-Intelligence-Integration:** Nutzung aktueller und historischer Bedrohungsdaten, einschließlich eigener TI-Feeds und kuratierter globaler Quellen, um Angriffe gezielt zu verhindern und auf die spezifischen Anforderungen des deutschen Mittelstands, der öffentlichen Hand und KRITIS zugeschnittene Abwehrmaßnahmen zu bieten [7] [13].
- **Passoptimierte Sicherheitsstrategien:** Entwicklung und Umsetzung von Maßnahmen, die vollständig an Kundenbedürfnisse und Risiken angepasst sind. Dies gewährleistet keine Übernahme fremder Konzepte, sondern passgenaue Lösungen auf lokaler Ebene [7] [21].
- **Compliance und Reporting:** Unterstützung bei der Einhaltung gesetzlicher und regulatorischer Vorgaben sowie Bereitstellung anpassbarer Berichte für unterschiedliche Stakeholder, inklusive Dashboards und kundenspezifischer Ansichten [13].
- **Skalierbarkeit und Flexibilität:** Sicherheitsdienste lassen sich an Größe und Komplexität der Kundeninfrastruktur anpassen, einschließlich Betrieb von eingebetteten SIEMs und Sensorik, ohne hohe Investitionen in eigene Ressourcen [7] [21].

Durch diese Fähigkeiten können MSSPs Cybersicherheit auf ein höheres Niveau heben, Risiken minimieren und gleichzeitig Kosten reduzieren – entscheidend in Zeiten von Fachkräftemangel und begrenzten IT-Sicherheitsbudgets.

Schlussfolgerung und Ausblick I

Die Bedrohungslage im Cyberraum entwickelt sich rasant – sowohl in Frequenz als auch in Komplexität. Besonders kritische Infrastrukturen, Behörden und Unternehmen mit hohen Compliance-Anforderungen sehen sich gezielten Angriffen ausgesetzt, die oft staatlich unterstützt werden und traditionelle Sicherheitsmaßnahmen umgehen können [4] [13].
Managed Detection and Response (MDR) in Kombination mit kontinuierlichem 24/7/365-Monitoring, souveräner Datenhaltung und bedarfsoptimierten Lösungen bietet einen klaren strategischen Vorteil.

Die Vorteile sind messbar:

- **Schnellere Erkennung** – bis zu 91 % aller Vorfälle innerhalb der ersten Stunde identifiziert [DCSO, 2025]
- **Verkürzte Verweildauer von Angreifern** – Reduktion um bis zu 70 % im Vergleich zu reaktiven Modellen
- **Signifikante Kostensenkung** – bis zu 45 % geringere Kosten pro Vorfall [28]
- **Compliance-Sicherheit** – DSGVO- und branchenspezifische Vorgaben werden konsequent eingehalten

Der Ausblick ist eindeutig: Die Rolle von KI in der Cyberabwehr wird weiter wachsen. Künftige MDR-Modelle werden verstärkt auf selbstlernende Systeme setzen, die Angriffe in Echtzeit vorhersagen, bevor sie überhaupt ausgeführt werden. Gleichzeitig bleibt die Kombination aus technischer Automatisierung und menschlicher Expertise der Schlüssel zur wirksamen Verteidigung.
Unternehmen, die heute in MDR investieren, schaffen sich nicht nur Schutz vor aktuellen Bedrohungen, sondern legen auch das Fundament für eine resiliente, zukunftsfähige IT-Sicherheitsarchitektur. Passoptimierte Strategien schaffen zudem Investitionssicherheit und ermöglichen die Weiternutzung bestehender Infrastruktur.

In einer Welt, in der Cyberangriffe längst ein permanentes Geschäftsrisiko darstellen, ist MDR nicht mehr optional – sondern ein unverzichtbarer Bestandteil moderner Unternehmensstrategie.

Schlussfolgerung und Ausblick II

Aspekt	Traditionelle Sicherheit	MSSP mit 24/7/365 & Icident Response
Erkennungsrate	63%	91%
Durchschnittliche Erkennungsrate	207 Tage	< 1 Stunde
Verweildauer von Angriffen	212 Tage	48 Tage
Reaktionszeit auf Vorfälle	Stunden bis Tage	Minuten (z.B. 9-20 Minuten)
Kosten	Höher durch interne Ressourcen	Bis zu 45% Kosteneinsparung
Skalierbarkeit	Begrenzte interne Kapazitäten	Hoch, flexibel anpassbar
Integration von Bedrohungsinformationen (Threat Intelligence)	Eingeschränkt	Voll integriert, aktuell und historisch
Nutzung von KI	Kaum bis gar nicht	Hoch, für Echtzeit-Analyse und Automatisierung

Über die DCSO

Deutsche Cyber-Sicherheitsorganisation GmbH

Die DCSO Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO) entwickelt moderne Cybersicherheits-Dienstleistungen für die deutsche Wirtschaft und bietet ihren Kunden darüber hinaus einen geschützten und herstellerneutralen Raum zum Austausch und der Zusammenarbeit in allen Fragen der Cybersicherheit. Unter dem Dach der DCSO tauschen sich Unternehmen nicht nur untereinander, sondern auch mit Behörden und Forschungsinstituten über Cybersicherheitsgefahren aus. Die gewonnenen Erkenntnisse fließen in effektive Strategien und Lösungen für Prävention, Reaktion sowie Abwehr und sorgen so für mehr Sicherheit für Unternehmen, Wirtschaft und Gesellschaft. Aus diesen Synergieeffekten der DCSO-Gemeinschaft und der eigenen Expertise entwickelt das Berliner Unternehmen moderne Managed Security Services in den Bereichen Bedrohungsidentifikation (Threat Intelligence), Überwachung und Detektion (Managed Detection & Response) sowie Hilfe zur Vorfallsbehandlung (Incident Response). Daneben unterstützt die DCSO Firmen mit Beratungsleistungen bei der Bewertung geeigneter Sicherheitstechnologien, der eigenen Cybersicherheit und der von Dienstleistern sowie beim Aufbau resilienter Business- und Informationssicherheitsprozesse. Mit dem Ziel der Bedrohungen durch global organisierte Cyberkriminalität und staatlich gelenkte Wirtschaftsspionage entgegenzuwirken, wurde die DCSO 2015 von Allianz SE, BASF SE, Bayer AG und Volkswagen AG für die deutsche Wirtschaft gegründet.

Unser Werteversprechen

Durch engste Verzahnung der eingesetzten Technologien ebenso wie durch personelle Rotation im Rahmen von Aus- und Weiterbildung zwischen allen Unternehmenseinheiten kann die DCSO Ende-zu-Ende-Cybersicherheit weit oberhalb des MSSP-Standards bieten: German Cybersecurity & Engineering - above and beyond!

Quellenverzeichnis

1. House Homeland Releases “Cyber Threat Snapshot” Highlighting Rising Threats to US Networks, Critical Infrastructure – Committee on Homeland Security. https://homeland.house.gov/2024/11/12/new-house-homeland-releases-cyber-threat-snapshot-highlighting-rising-threats-to-us-networks-critical-infrastructure/
2. Bundesamt für Sicherheit in der Informationstechnik (BSI). Cybernation. https://www.bsi.bund.de/DE/Das-BSI/Cybernation/cybernation_node.html
3. The Rise of Zero-Day Vulnerabilities: Why Traditional Security Solutions Fall Short. https://thehackernews.com/2024/10/rise-of-zero-day-vulnerabilities.html
4. Secure Cyberspace and Critical Infrastructure | Homeland Security. https://www.dhs.gov/archive/secure-cyberspace-and-critical-infrastructure
5. Managing the Risks of China’s Access to U.S. Data and Control of Software and Connected Technology | Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en
6. The Limitations Of Traditional Security Measures - FasterCapital. https://fastercapital.com/topics/the-limitations-of-traditional-security-measures.html
7. McKinsey. AI is the greatest threat—and defense—in cybersecurity today. Here’s why. https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-is-the-greatest-threat-and-defense-in-cybersecurity-today
8. ScienceDirect. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. https://www.sciencedirect.com/science/article/pii/S2543925123000372
9. Fortinet. Artificial Intelligence (AI) in Cybersecurity: The Future of Threat Defense. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity
10. Belfer Center for Science and International Affairs. Attacking Artificial Intelligence: AI’s Security Vulnerability and What Policymakers Can Do About It. https://www.belfercenter.org/publication/AttackingAI
11. The Economic Times. China could shut US power grid, gas pipelines and electrical networks at will with killswitch, says shocking report. https://economictimes.indiatimes.com/news/international/us/china-could-shut-us-power-grid-gas-pipelines-and-electrical-networks-at-will-with-killswitch-says-shocking-report/articleshow/123121296.cms
12. Chinaobservers. China Holds a Kill Switch to European Power Grids. https://chinaobservers.eu/china-holds-a-kill-switch-to-european-power-grids/
13. BSI. Lagebericht zur IT-Sicherheit in Deutschland. https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html
14. Heise Security. Aktuelle Bedrohungslage. https://www.heise.de/security/
15. BMI. Cyber-Sicherheitsstrategie für Deutschland. https://www.bmi.bund.de/DE/themen/it-internet/cybersicherheit/cybersicherheit-node.html
16. FAZ. Neue Bedrohungslage: Wie KI unsere Cybersicherheit beeinträchtigt. https://www.faz.net/aktuell/wirtschaft/digitec/neue-bedrohungslage-wie-ki-unsere-cybersicherheit-beeintraechtigt-19084610.html

17. FAZ. IT-Sicherheit: Cyberkriminelle nutzen immer häufiger KI als Waffe. https://www.faz.net/aktuell/feuilleton/medien-und-film/it-sicherheit-cyberkriminelle-nutzen-immer-haeufiger-ki-als-waffe-110621925.html

18. BSI. Die Lage der IT-Sicherheit in Deutschland 2024. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html

19. Bundeswehr. Bedrohung Russland im Cyber- und Informationsraum. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/bedrohung-russland-cyber-informationsraum-5981306

20. Bitkom. Leitfaden „Generative KI im Unternehmen". https://www.bitkom.org/Bitkom/Publikationen/Generative-KI-im-Unternehmen

21. Deutscher Bundestag. Inforbrief Juli 2025: Zu rechtlichen Vorgaben der Verordnung über Künstliche Intelligenz für den Einsatz von KI in Behörden der EU-Mitgliedsstaaten. https://www.bundestag.de/resource/blob/1098992/ki-einsatz-in-behoerden-der-eu-staaten.pdf

22. BusinessWire. GenLab Venture Studios and DCSO Announce a Strategic Partnership and Investment to Launch a Venture Studio Building Next-Generation Agentic AI Cyber Defense. https://www.businesswire.com/news/home/20250304559870/en/GenLab-Venture-Studios-and-DCSO-Announce-a-Strategic-Partnership-and-Investment-to-Launch-a-Venture-Studio-Building-Next-Generation-Agentic-AI-Cyber-Defense

23. FAZ. Großbritannien schließt Huawei von 5G-Ausbau aus. https://www.faz.net/pro/digitalwirtschaft/grossbritannien-schliesst-huawei-von-5g-ausbau-aus-16860481.html

24. Bloomberg Podcast. Trump Announces Fighter Jet Deal for Boeing: Full Remarks. https://www.bnnbloomberg.ca/business/company-news/2025/03/21/eyeing-china-threat-trump-announces-boeing-wins-contract-for-secretive-future-fighter-jet/

25. DCSO Whitepaper. Threat Detection & Hunting: Cyberangriffe auf Stadtwerke und lokale Versorger abwehren.

26. Nebulex Pty Ltd., Australia. The ROI of Managed Security Services: Enterprise Case Studies.

27. Gartner. 72 % der Unternehmen benötigen maßgeschneiderte Sicherheitslösungen. „Market Guide for Managed Security Services" (2023).

28. Deloitte. MSSP-Lösungen können die Gesamtkosten für Cybersicherheit um bis zu 45 % senken. „Cost Optimization in Cybersecurity" (2022).

29. IBM Security. Erkennungsrate von Sicherheitsvorfällen auf 95 % gesteigert. „Cost of a Data Breach Report" (2024).

30. PwC Deutschland. Sicherheitskosten um 40 % gesenkt (Fallbeispiel Gesundheitssektor). „Healthcare Cybersecurity Case Study" (2023).

31. Bitkom. 89 % der deutschen Unternehmen wünschen sich „Made in Germany"-Lösungen. „Digitale Souveränität in der deutschen Wirtschaft" (2024).

32. Fraunhofer IAO. Lokale Datenspeicherung kann Compliance-Kosten um bis zu 35 % reduzieren. „Kostenanalyse digitaler Souveränität" (2023).

33. Roland Berger. Compliance-Kosten um 30 % gesenkt (Fallbeispiel Automobilhersteller). „Cybersecurity in der Automobilindustrie" (2023).

34. BSI. Reaktionszeiten auf Sicherheitsvorfälle von 48 Stunden auf unter 2 Stunden reduziert. „Lagebericht zur IT-Sicherheit in Deutschland" (2024).

35. BSI. Liste der qualifizierten APT-Response-Dienstleister; Stand: 31.07.2025. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

36. Bundeswehr – Kommando CIR Cyber und Informationsraum. Cyber- und Informationsraum: KI – Künstliche Intelligenz – Die unsichtbare Superkraft der Zukunft. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum

DCSO
Deutsche Cyber-Sicherheitsorganisation GmbH
EUREF-Campus 22
10829 Berlin, Germany

+49 30 - 72 62 19 - 0
info@dcso.de

www.dcso.de